FIŞA DISCIPLINEI

Tehnici de calcul cuantice cu aplicaţii în criptografie şi IA

Anul universitar 2025-2026

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeş-Bolyai
1.2. Facultatea	Facultatea de Matematică şi Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Licenţă
1.6. Programul de studii / Calificarea	Informatică
1.7. Forma de învățământ	Cu frecvenţă

2. Date despre disciplină

2.1. Denumirea disciplinei	**Tehnici de calcul cuantice cu aplicaţii în criptografie şi IA**					Codul disciplinei	**MLE5216**
2.2. Titularul activităților de curs	Lector Univ. dr. Mihoc Tudor Dan						
2.3. Titularul activităților de seminar	Lector Univ. dr. Mihoc Tudor Dan						
2.4. Anul de studiu	6	2.5. Semestrul	2	2.6. Tipul de evaluare	C	2.7. Regimul disciplinei	Opțional

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Număr de ore pe săptămână	**5**	din care: 3.2. curs	**2**	3.3. seminar/ laborator /proiect	**0/1/2**
3.4. Total ore din planul de învățământ	60	din care: 3.5. curs	24	3.6 seminar/laborator /proiect	**0/12/24**
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					**ore**
Studiul după manual, suport de curs, bibliografie și notițe (AI)					24
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					16
Tutoriat (consiliere profesională)					2
Examinări					3
Alte activități					0
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)					**65**
3.8. Total ore pe semestru					**125**
3.9. Numărul de credite					**5**

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Cunoștințe de bază de Analiză și Algebră liniară.
4.2. de competențe	Cunoștințe de bază de programare în Python.

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Proiector.
5.2. de desfășurare a seminarului/ laboratorului	Laborator cu calculatoare. Software: Anaconda, Python, Qiskit.

6.1. Competențele specifice acumulate[1]

Competențe profesionale /esențiale	• programarea în limbaje de nivel înalt; • dezvoltarea și întreținerea aplicațiilor informatice; • utilizarea instrumentelor informatice în context interdisciplinar;
Competențe transversale	• aplicarea regulilor de muncă organizată şi eficientă, a unor atitudini responsabile faţă de domeniul didactic-ştiinţific, pentru valorificarea creativă a propriului potenţial, cu respectarea principiilor şi a normelor de etică profesională; • desfăşurarea eficientă a activităţilor organizate într-un grup interdisciplinar şi dezvoltarea capacităţilor empatice de comunicare interpersonală, de relaţionare şi colaborare cu grupuri diverse; • utilizarea unor metode şi tehnici eficiente de învăţare, informare, cercetare şi dezvoltare a capacităţilor de valorificare a cunoştinţelor, de adaptare la cerinţele unei societăţi dinamice şi de comunicare în limba română și într-o limbă de circulație internațională;

6.2. Rezultatele învățării

Cunoștințe	• Absolventul are cunoștințe necesare pentru utilizarea calculatoarelor, dezvoltarea programelor și aplicațiilor software, procesarea informațiilor; • Absolventul are abilitatea de a dezvolta, proiecta și crea noi aplicații, sisteme sau produse folosind bunele practici din domeniu; • Absolventul are aptitudinile necesare pentru conceperea programelor de calculator și analiza sistemelor software; • Absolventul este capabil să identifice probleme complexe și să examineze probleme conexe pentru a dezvolta opțiuni de rezolvare și implementa soluții; • Absolventul are abilitatea de a aplica reguli generale unor probleme specifice și de a produce soluții relevante;
Aptitudini	• Absolventul are abilitatea de a aplica reguli generale unor probleme specifice și de a produce soluții relevante; • Absolventul este capabil să combine informații diverse pentru a formula soluții și genera idei de dezvoltare pentru noi produse și aplicații; • Absolventul are cunoștințe legate de programare, matematică, inginerie și tehnologie si are abilitățile necesare pentru a le folosi in crearea de sisteme informatice complexe;
Responsabilități și autonomie	• Absolventul are abilitatea de a înțelege și comunica eficient informațiile; • Absolventul are cunoștințele necesare pentru selectarea și utilizarea procedurilor potrivite de instruire pentru a facilita procesul de asimilare a cunoștințelor; • Absolventul este capabil de a prezenta și a explica metodele, algoritmii, paradigmele si tehnicile folosite în diferite ramuri ale informaticii;

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	• Scopul este de a oferi studenților o înțelegere cuprinzătoare a calculului cuantic, încurajând în același timp curiozitatea, și gândirea critică, motivându-i de a se implica în acest domeniu interdisciplinar de ultimă generație.
7.2 Obiectivele specifice	• Obiectivul este de a oferi studenților o înțelegere cuprinzătoare a principiilor, tehnicilor și aplicațiilor calculului cuantic în două domenii cheie: criptografia și inteligența artificială (IA).

8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Introducere – premise matematice	Expoziție; Dialog;	

[1] Se poate opta pentru competențe sau pentru rezultatele învățării, respectiv pentru ambele. În cazul în care se alege o singură variantă, se va șterge tabelul aferent celeilalte opțiuni, iar opțiunea păstrată va fi numerotată cu 6.

2. Noțiuni fundamentale de calcul cuantic (Qubiți și Sfera Bloch)	Prezentare; Expunere interactivă;	
3. Porți Quantice. Circuite cuantice		
4. Fenomenul de fază kick-back		
5. Algoritmi de căutare cuantică		
6. Algoritmul lui Schor		
7. Criptografie cuantică și criptografie post-cuantică. Atacuri prin calcul cuantic asupra RSA		
8. Distribuția cheilor cuantice (QKD). Zgomot în QKD (eyedropper)		
9. Clusterizare în calculul cuantic		
10. Quantum Pattern Recognition		
11. Clasificarea cuantică		
12. Regresia cuantică		
Bibliografie 1. Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information." (2002): 558-559. 2. Gisin, Nicolas, et al., "Quantum cryptography." Reviews of modern physics 74.1 (2002): 145. 3. Yan, Song Yuan. “Cryptanalytic attacks on RSA.” (2007). 4. Bruß, Dagmar, and Norbert Lütkenhaus. "Quantum key distribution: from principles to practicalities." Applicable Algebra in Engineering, Communication and Computing 10.4 (2000): 383-399. 5. Shor, Peter W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332. 6. P. Wittek, Quantum machine learning: what quantum computing means to data mining, Academic Press, Elsevier, 2014. 7. S. D. Sarma, D. Dong-Ling, and D. Lu-Ming, Machine learning meets quantum physics, arXiv preprint arXiv:1903.03516, 2019.		
8.2 Seminar / laborator	Metode de predare	Observații
1. Generatoare cuantice de numere aleatoare	Exemplu; Implementarea algoritmilor;	
2. Transformata Fourier cuantică		
3. Algoritmul lui Deutsch. Algoritmul lui Deutsch–Jozsa.		
4. Algoritmul de căutare al lui Grover.		
5. Algoritmul cuantic de factorizare.		
6. Algoritmul cuantic pentru logaritmi discreți.		
7. Rețele neuronale cuantice.		
Bibliografie 1. Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information." (2002): 558-559. 2. Gisin, Nicolas, et al., "Quantum cryptography." Reviews of modern physics 74.1 (2002): 145. 3. Yan, Song Yuan. “Cryptanalytic attacks on RSA.” (2007). 4. Bruß, Dagmar, and Norbert Lütkenhaus. "Quantum key distribution: from principles to practicalities." Applicable Algebra in Engineering, Communication and Computing 10.4 (2000): 383-399. 5. Shor, Peter W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332. 6. P. Wittek, Quantum machine learning: what quantum computing means to data mining, Academic Press, Elsevier, 2014. 7. S. D. Sarma, D. Dong-Ling, and D. Lu-Ming, Machine learning meets quantum physics, arXiv preprint arXiv:1903.03516, 2019.		

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Cursul urmează schema și structura utilizate de cele mai importante universități din SUA și Europa;
- Cursul există în programele de studiu ale unor universități importante din străinătate.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Studenții trebuie să fie capabili să exemplifice și să utilizeze concepte de bază și avansate ale calculului cuantic.	colocviu	50%
10.5 Seminar/laborator	Studenții trebuie să fie capabili să implementeze algoritmii descriși în curs și discutați în cadrul demonstrațiilor din cadrul laboratoarelor.	evaluarea temelor de laborator	50%
10.6 Standard minim de performanță			
● Cel puțin nota 5 (pe o scală de la 1 la 10) pentru ambele tipuri de evaluare.			

11. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)[2]

Nu se aplică.

Data completării:
15.04.2025

Semnătura titularului de curs

Lector Univ. Dr. Mihoc Tudor Dan

Semnătura titularului de seminar

Lector Univ. Dr. Mihoc Tudor Dan

Data avizării în departament:
...

Semnătura directorului de departament

Conf. Dr. Adrian STERCA

[2] Păstrați doar etichetele care, în conformitate cu *Procedura de aplicare a etichetelor ODD în procesul academic*, se potrivesc disciplinei și ștergeți-le pe celelalte, inclusiv eticheta generală pentru *Dezvoltare durabilă* - dacă nu se aplică. Dacă nicio etichetă nu descrie disciplina, ștergeți-le pe toate și scrieți "*Nu se aplică.*".